The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
06/15/2011

SUBJECT:
Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (MS11-041)

OVERVIEW:
A vulnerability has been discovered in Microsoft Windows that could allow for remote code execution when handling specially crafted OpenType fonts. OpenType fonts are fonts that are embedded in documents such as Microsoft Word or used in web pages. The vulnerabilities can be exploited if a user visits a network share containing a specially crafted OpenType font. This vulnerability can also be exploited if a user views a specially crafted OpenType font using a web browser linked to a network share. Successful exploitation of these vulnerabilities could result in an attacker gaining system-level privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Windows XP x64
- Windows Server 2003 x64
- Windows Server 2003 Itanium-based systems
- Windows Vista x64
- Windows 2008 x64
- Windows 2008 Itanium-based systems
- Windows 7 x64

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: **High**

DESCRIPTION:
A vulnerability in Microsoft Windows Kernel-mode driver could allow for remote code execution due to improper parsing of specially crafted OpenType fonts. This vulnerability is caused by the Windows Kernal-mode driver not properly validating pointers while parsing OpenType fonts. This vulnerability specifically impacts the win32K.sys component of Windows systems. This vulnerability can be exploited through the following attack scenarios.

In a web-based attack scenario, an attacker could host a web site that contains a link to a network share containing a specially crafted OpenType

font. When the user navigates to the web site, the affected control path is triggered via the Details and Preview panes in Windows Explorer.

In a network-based attack scenario, an attacker could host a specially crafted OpenType font on a network share. When the user navigates to the share in Windows Explorer, the affected control path is triggered via the Details and Preview panes in Windows Explorer.

Successful exploitation of this vulnerability could allow an attacker to run arbitrary code in kernel mode and take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

It should be noted that this vulnerability only affects x64-based and Itanium-based versions of Windows operating systems; 32-bit versions of Windows operating systems are not affected.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the principle of Least Privilege to all services.
- Consider disabling the WebClient service if there is no documented business need.
- Implement egress and ingress filtering for TCP ports 139 and 445 at your network perimeter.

REFERENCES:

Microsoft:

http://www.microsoft.com/technet/security/Bulletin/ms11-041.mspx

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1873

Securityfocus:

http://www.securityfocus.com/bid/48183/